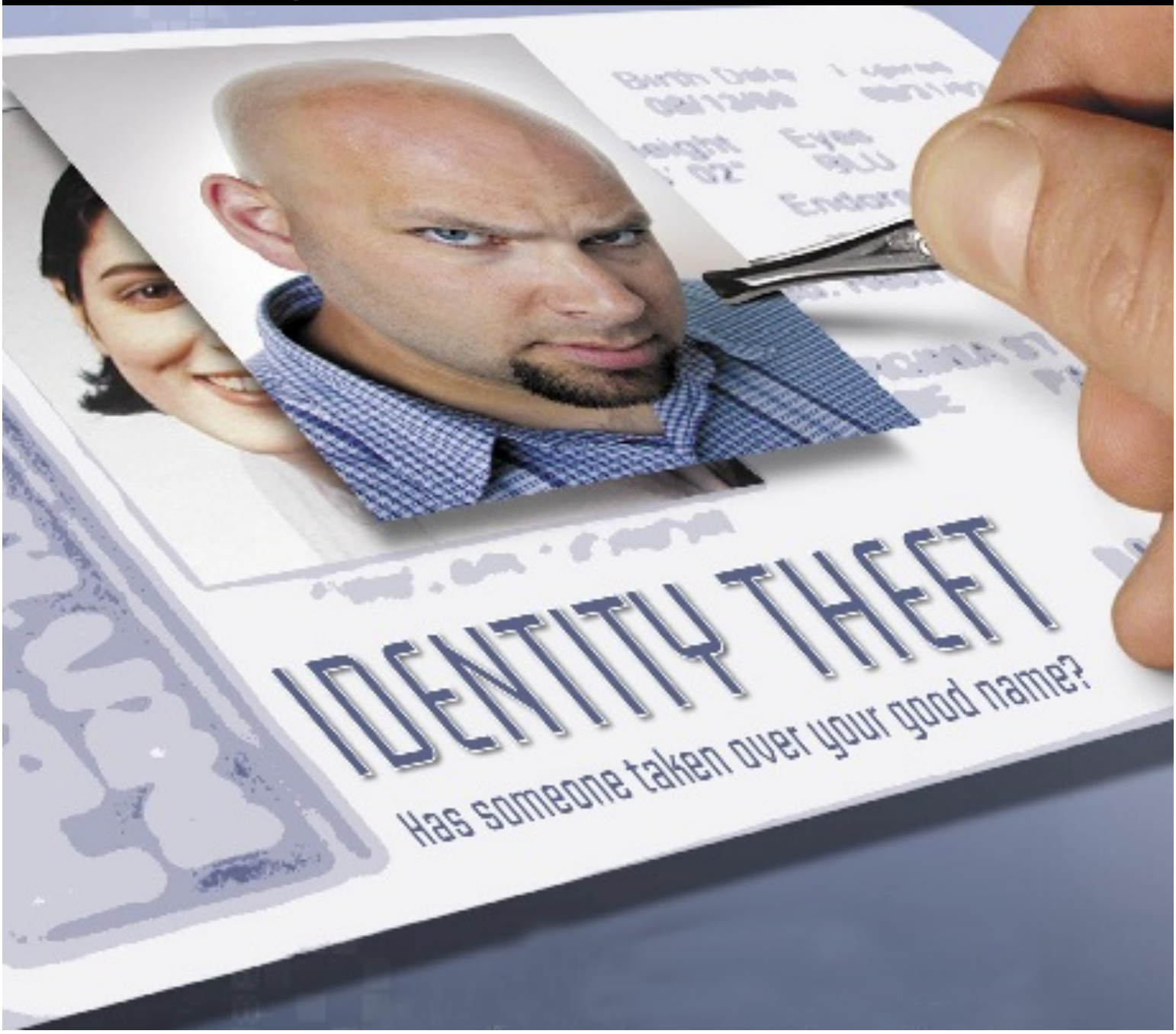
**Tim Dobeck**
Parma Law Director/
Chief Prosecutor

## Protecting Yourself Against

# Identity Theft



## General Background

Since the 1990s, Identity Theft has become one of the fastest growing crimes in America. The crime of Identity Theft occurs when a criminal obtains and uses a consumer's sensitive personal identifying information to purchase goods or services fraudulently. Examples of personal identifying information include credit card numbers, bank account numbers, insurance information, income information (pay stubs), Social Security Number, or even the consumer's name, address and telephone number(s).

Generally, an identity thief will commit identity theft by either:

1. Using your personal identifying information to directly purchase goods or services; or

2. More likely, use your personal identifying information to apply for and obtain new lines of credit in your name, then use this credit to purchase goods and/or services and leaving you the victim to pay the bill.

   In this example, the victim usually will not discover the fraudulent use of their personal identifying information until they are turned down for credit, or they begin to receive calls from unknown creditors demanding payment for goods and/or services they never purchased. By the time the victim learns of the fraudulent use of their personal identifying information, the victim's good name and credit record will have been ruined. Worst yet, identity thieves may present the victim's identifying information during traffic stops or when they are arrested for a crime – leaving the innocent victim subject to warrants issued in their name.

A point to remember is that the stock in trade of identity thieves is your everyday transaction. Every time you perform a transaction, your personal identifying information is at risk of being intercepted or obtained by identity thieves. YOU MUST TAKE STEPS TO PROTECT YOUR PERSONAL IDENTIFYING INFORMATION (BE PROACTIVE AND VIGILANT AGAINST IDENTITY THEFT).

Another very important point to remember is that you do not have to be alive to be a victim of identity theft.

## Statistics

- The most recent data available from the Federal Trade Commission asserts that approximately 8.4 Million Americans have fallen prey to some form of identity theft scam in 2007, costing businesses and victims combined $49.5 Billion dollars in losses.
- 246,035 complaints alleging identity theft were filed with the Federal Trade Commission in 2007.
- 6,878 cases of identity theft in Ohio were reported to the Federal Trade Commission in 2007, 8th most in the United States.
- The median value of goods and services obtained by identity thieves since 2001 is approximately $500. The mean loss total per victim of identity theft in 2007 is $5,720.
- The average time it takes a victim of identity theft to correct the harm done by an identity thief in 2007 is 5 hours. The mean time for resolution is 25 hours.
- Between 2001-2006, the most extreme cases of identity theft have required up to 130 hours per victim to be resolved.
- 62% of victims of identity theft in 2007 did not notify the crime to the police.

## News on Identity Theft

- **ChoicePoint (2004)** – The largest information broker in the United States disclosed in a Securities and Exchange Commission filing that criminals posing as legitimate small businesses obtained the personal data of approximately 145,000 people listed in the ChoicePoint database.
- **Bank of America (2005)** – Disclosed that it lost digital tapes containing credit card account records of 1.2 Million federal employees, including 60 United States Senators.
- **CardSystems Solutions (June 2005)** – A cyber security breach at the Atlanta based payment processing company exposed the data of more than 40 million credit card accounts to fraud.
- **Wells Fargo (May-June 2008)** – A Wells Fargo bank access code was used to steal the personal information of approximately 5,000 consumers.
- **Countrywide Home Loans (August 2008)** – A senior financial analyst at the company's sub prime mortgage division is arrested on charges that he sold the personal information of loan applicants to third parties over a period of two years.
- **Walnut Creek, California (September 2008)** – Approximately 75,000 accounts with sensitive information are at risk after a human resources outsourcing company was robbed over the Memorial Day weekend.

# Laws on Identity Theft

## Ohio Laws

The State Assembly has passed laws which address the growing problem of identity theft. Ohio's identity theft law (Ohio Revised Code § 2913.49), which went into effect on August 25, 1999, makes it a crime to intentionally use another person's identifying information to fraudulently obtain credit, property, or services. ORC § 2913.49 also takes into account computer and Internet technology, and furthermore makes it a crime to aid or abet another person in fraudulently obtaining personal identifying information of a third person.

The Ohio Attorney General's Office has unveiled the Identity Theft Verification Passport program in December 2004. Under this unique program, victims of identity theft are issued a *PASSPORT* card which will conclusively demonstrate to law enforcement authorities and creditors alike that their identity has been stolen. (Additional details on PASSPORT program given below)

## Federal Laws

Ohio's identity theft law (§ 2913.49) is modeled after the Identity Theft and Assumption Deterrence Act, enacted by the United States Congress in October 1998 (and codified at 18 USC § 1028). Violations of the Act are investigated by federal agencies, including the Secret Service, the FBI, and the United States Postal Inspector. Violations are prosecuted by the US Department of Justice. In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit identity theft.

Under Federal law/rules, your liability for unauthorized checking transactions and credit card transactions is set at a maximum of $50 so long as you report the unauthorized transaction within 30 days of receiving you checking statement and within 60 days of receiving your credit card statement. In regard to electronic funds transfers/online banking problems, you will be liable for up to $50 if you report the problem within 2 days of its event, and up to $500 if you report the problem within 60 days of its event.

Unfortunately, even with the enactment of these stringent laws, identity theft is still occurring at record levels. The bottom line is that, as with any crime, it is impossible for the government to completely eliminate identity theft. It is also impossible for you to completely control whether you become a victim of identity theft. You can, however, minimize your risk by managing your personal identifying information cautiously and with heightened sensitivity.

## How Identity Theft Occurs

Before you can take the appropriate steps to protect your personal identifying information, you must first understand the methods that identity thieves employ in obtaining your sensitive data. Identity theft ranges from simple theft to new and innovative techniques used to intercept your personal identifying information through electronic means. The following is a non-exhaustive list of the many forms that identity theft takes:

- Rummaging or "dumpster diving" through trash looking for billing and banking statements, pre-approved credit card offers, credit and bank cards which often include Social Security numbers, bank account and credit card numbers in addition to home addresses and telephone numbers. Remember – there is no expectation of privacy in trash placed on your tree lawn for collection.
- Stealing wallets and purses containing identification, credit cards and bank cards.
- Stealing personal identifying information directly from your own home.
- Stealing mail, most often from the victim's own mailbox, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- Re-Shipping Scheme – Thieves convince others to receive their personal mail for them. Victim is then arrested for receiving illegal goods. Remember – never accept mail for someone you don't know and trust. Also, you have the right to refuse delivery of anything.
- Fake Check Scam – The victim will be selling something, usually a big-ticket item. The victim is contacted by someone usually from overseas who is allegedly interested in purchasing victim's item. After agreeing to purchase the item, the identity thief will send the victim a fake cashier check for an amount greater than the price of the item and will ask the victim to wire them the difference.
- The identity thief will complete a "change of address" form to divert the victim's mail to another location.
- The identity thief will scam personal identifying information from the victim by posing as a legitimate business person or government official.
- The identity thief will obtain personal identifying information from businesses or financial institutions by stealing records, bribing an employee ("inside source") who has access to consumer records, or hacking into the business' computer database.
- The identity thief will obtain credit reports by using his/hers employer's authorized access to credit reports or by posing as a landlord, employer, or someone else who may have a legal right to the personal identifying information.
- The identity thief will pose as a telemarketer or a customer service representative from a legitimate business over the telephone and ask questions with the intent to obtain personal identifying information.
- Call Forwarding Scams – Dialing provided codes will transmit your telephone account information over the telephone to the identity thief. (further details ahead)

- Skimming – The identity thief will steal credit and debit card numbers as the victim's card is processed by using a special information storage device.
- Modem Hijacking – A virus is sent over telephone line, crashing the victim's modem. The victim will then be prompted to reconnect using new dial-up numbers which unknown to the victim are long distance numbers. (Further details ahead)
- The identity thief will intercept personal identifying information the victim transmits through an unsecured Internet side.

## After Your Identity Has Been Stolen

Once identity thieves obtain your personal identifying information, they may fraudulently use your data in a variety of ways. Some of the most common fraudulent uses include:

- Go on spending sprees using the victim's credit and/or debit card account numbers to buy big ticket items such as computers and other expensive electronic equipment that may be easily sold to unsuspecting third parties.
- Open a new credit card account, using the victim's name, date of birth, and Social Security number, and maxing out such credit. When the bills are not paid, the delinquent account is reported on your credit report.
- Change the mailing address on the victim's credit card account. The identity thief then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before the victim realizes that there is a problem.
- Use personal identifying information to take out loans in the victim's name.
- Establish telephone or wireless service in the victim's name.
- Attempt to use your credit card to make an overseas telephone call.
- Counterfeit checks or debit cards, and drain the victim's account.
- Open a bank account in the victim's name and proceed to write bad checks on that fraudulent account.
- File for bankruptcy under the victim's name to avoid paying debts that the thief has incurred, or to avoid eviction.
- Give the victim's name to the police during an arrest. Once the identity thief fails to show for his/her court date, an arrest warrant will be issued in the unsuspecting victim's name.

## How To Tell If You Are a Victim of Identity Theft

Although indicators of identity theft can be the result of a simple error, consumers should never assume that there has been a mistake and do nothing. Always follow up with the business or institution to find out the reason behind the error. Some common indicators of identity theft include the following:

- Monitor balances of financial accounts on a regular basis. Look for unexplained charges or withdrawals.
- Failing to receive bills or other mail signaling an address change has been performed by the identity thief.
- Receiving credit card for which you did not apply.
- Denial of credit for no apparent reason.
- Receiving calls from debt collectors or companies about merchandise or services you did not purchase.

## Protecting Yourself Against Identity Theft

Magazines, credit card companies, clubs, organizations, charities, manufacturers, and retailers make lists of their subscribers, customers, members, and donors available to other businesses for a fee. Your personal identifying information and financial data is reproduced and sold in countless ways and often without your knowledge.

An ounce of prevention is worth its weight in gold, especially in today's digitized society. It is far easier to prevent identity fraud than to repair the damage that is done by criminals who want to steal your identity. The following tips can help you better secure your personal identifying information.

### General Protections

- Keep all personal identifying information and financial data stored in a secure place. If you haven't done so, consider purchasing a safe.
- Carry sensitive identifying information in a close fitting pouch or in your front pocket, NOT in your purse or wallet, including driver's license, credit & debit cards, checks, car registration and anything with your Social Security Number (make a copy of your Medicare card and black out all but the last four digits.)
- Do not keep your purse, briefcase, checkbook, registration, insurance card, or other identifying information in your car. Carry them in a secure manner on your person.
- Copy the contents (front and back) of your wallet.
- Order a free copy of your credit report from each of the three (3) credit reporting agencies (Experian, Equifax, TransUnion) every year. You may contact the three bureaus directly or by going to www.annualcreditreport.com or calling (877) 322-8228. Do NOT use www.freecreditreport.com.

- Register with Direct Marketing Association to opt-out of most marketing lists by calling (888) 5 OptOut (567-8688) or going online at www.dmachoice.org.
- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Also, ask about disposal procedures for those records.
- Visit the Federal Trade Commission Website www.ftc.gov/idtheft for more information about preventing and dealing with identity theft.

**PAPER MAIL/HARD RECORDS**

- Thoroughly shred financial record and statements you are disposing of using a cross shredder.
- In a similar vein, take all ATM receipts home and cross shred them.
- If they have not already done so, request that your bank remove account numbers from ATM receipts.
- Carefully review your monthly bills to ensure no fraudulent charges have been made on your account.
- Do not leave outgoing bill payments in your home mailbox. Deposit mail directly into a secure USPS mail receptacle.
- If you're planning to be away from home and cannot arrange for your mail to be picked up, call the United States Postal Service at (800) ASK-USPS (275-8777) or go online at www.usps.com to request a vacation hold.
- Read the fine print of any document you sign or provide information on.
- Avoid receiving junk mail solicitations or pre-approved credit cards by registering with Direct Marketing Association at www.dmachoice.org or submitting a registration form to: Mail Preference Service; Attn. Dept. 27478505; Direct Marketing Association; P.O. Box 282; Carmel, New York 10512. Within 90 days of receiving your request, approximately 70% of national direct marketers will delete your name and address from their marketing list. The registration will be good for three (3) years.

**CREDIT CARDS/ATM CARDS**

- Reduce the amount of credit cards you actively use to a maximum of two.
- Destroy all credit cards and ATM cards that you do not actively use.
- Always take credit card receipts with you. Never toss them in a public trash container.
- Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded in your credit report which is full of personal data that can be used by identity thieves.
- Immediately contact the issuer of your credit cards if a credit card you are expecting does not arrive.
- When making a credit card purchase from a retailer, ask for credit card carbons if the retailer is not using carbonless forms.
- Request (in writing) that the issuer for each of your credit cards remove your name from marketing and promotional lists that may be sold to or shared with other companies.

- Request (in writing) that the issuer of your credit cards remove your name from mailing lists used to provide you with random issue convenience checks. Credit Card convenience checks are easy prey for identity thieves to steal and use. Often, the consumer is unaware that the checks were ever issued.
- Stop annoying credit card solicitations by calling the Credit Reporting Industry Opt-out toll-free number (888) 567-8688 to have the 3 credit bureaus block your credit files from credit card companies. You may also opt-out from credit card solicitations through www.optoutprescreen.com.

**SOCIAL SECURITY NUMBER**

- Do not carry you Social Security card with you. Keep it in a secure place. Your Social Security Number is the key to your banking and credit card accounts, as well as your insurance and health benefits, making it a prime target of identity thieves.
- Omit your Social Security Number from all documents and licenses that do not legally require your number. Ohio driver's license omits SSN by default. SSN no longer indicated on your tax refund since January 2004.
- Check your earnings statement for discrepancies (statement received every year three (3) months before your birthday. Contact the Social Security Administration and ask for Form SSA-7004, *Request for Earnings and Benefit Estimate Statement* (it's free and there is no limit to how often you may request it.)
- If you believe an identity thief is using your Social Security Number, call the Social Security Fraud Hotline at (800) 269-0271.

**TELECOMMUNICATIONS**

- Never provide personal identifying information or financial date over the telephone if you did not initiate the contact.
- Beware of anyone calling to "confirm" personal or financial information.
- Do not agree to any sale or offer over the telephone when the call is unsolicited and you do not know the caller or company. Ask that promotional materials be mailed to you instead.
- Do not be intimidated by callers who suggest dire consequences if you do not immediately provide or verify your financial information.
- If the caller initiates the contact, ask that he/she identifies themselves. If the caller refuses, hang up immediately.
- If the caller initiates the contact and provides his/her identity, ask the caller for his/her contact information so that you can call them directly and verify they are who they claim to be.
- Simply hang up or delete any voicemail message if someone calls asking you to dial a series of numbers.
- Carefully review your telephone bill each month to make sure your long distance carrier has not been switched without your authorization.
- Before making any purchase or donation over the telephone, contact you local Better Business Bureau (http://cleveland.bbb.org) or Attorney General's Office (https://agcares.ag.state.oh.us/public/search.aspx) to check on the company's business and complaint history.

- Report suspicious calls immediately to the Federal Trade Commission at either (877) IDTHEFT (438-4338) or www.ftc.gov/idtheft.
- Remove your name from all telephone directories.
- Receive fewer unsolicited telemarketing calls by registering both your home and cellular telephone numbers with the National Do Not Call Registry at www.donotcall.gov (you will need an email to register) or call (888) 382-1222 from the phone you want to register.

**EMAIL/INTERNET** (*Your computer can be a gold mine of personal information to an identity thief*)

- Do not store financial information on your computer unless absolutely necessary. If you do, use a "strong" password – combination of letters (upper and lower case), numbers and symbols.
- Delete of any personal information stored on your computer before you dispose of it. Use a drive erasing utility that overwrites the entire hard drive and makes files unrecoverable.
- Use a secure browser to guard the safety of online transactions. When submitting information, look for a "lock" icon on the status bar (confirms security during transmission).
- Avoid using automatic log-in features that stores your user name and password. Always log off when finished.
- Verify the security of a website before making any online purchase. Never transmit personal identifying information or financial data via email or an website that is not secure.
- Never click on links provided in an email you believe fraudulent. It may contain a virus that can contaminate and compromise your computer.
- If you believe an email to be legitimate, go to the company's website by typing the IP address directly or using your favorites instead of using the link that is provided in the email.
- Obtain and update regularly virus and spyware scanning software for all your computers to protect your computer against these types of malicious programs.
- Use a firewall especially if you have a high speed or "always on" connection. The firewall allows you to limit uninvited access to your computer. Without a firewall, hackers can take over your computer and access sensitive information.
- Look for security repairs and patches you can download from your operating system's website.
- Do not download files from strangers or click on hyperlinks from people you don't know. Doing so may cause your modem to be hijacked, or even worse, giving control of your computer to an identity thief.
- Go to http://scamorama.com to get the latest news and information on scams.
- Report suspicious emails immediately to the Federal Trade Commission at either (877) IDTHEFT (438-4338) or www.ftc.gov/idtheft.
- Reduce the amount of unsolicited email you receive by visiting www.dmachoice.org and place an online request. Requests are usually good for one year.
- If you get spam email that you think is deceptive, forward it to spam@uce.gov.

**PASSWORDS & PERSONAL IDENTIFICATION NUMBERS (PINS)**

- When creating passwords or PINS, do not use the last 4 digits of your SSN, DOB, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could be discovered easily by thieves.
- Ask financial institutions to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use easily discoverable passwords or PINS.
- Discourage your bank from using the last 4 digits of your Social Security Number as your assigned PIN.
- Memorize all your passwords and PINS. Do not record them on anything in your wallet or purse.
- Shield your hand when using your PIN at an ATM or when making long distance phone calls with your telephone calling card to prevent others from seeing your secret code.

## WHAT YOU SHOULD DO IF YOU ARE A VICTIM OF IDENTITY THEFT

You should take the following 4 steps right away: (*Remember to follow up all calls in writing; send letters by certified mail, return receipt requested, so that you can document what the company received and when; and keep copies in your file*)

### ☑ Police Report

File a report of the identity theft with your local police or the police in the jurisdiction where the identity theft took place. (Get a copy of the report for your records, or at the very least, get a report number as a reference). You should also send a copy of the police report to your bank, credit-card company, and insurance company. Some tips on filing a police report include the following:

✓ Provide documentation – Furnish as much relevant documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report.

✓ Be persistent – If you're told that the identity theft is not a crime under state law, ask to file a Miscellaneous Incident Report instead.

✓ Be a motivating force – Ask your police department to search the FTC's Consumer Sentinel database for other complaints in your community. You may not be the first victim in your community and helping authorities discover a pattern will lead local authorities to give your case added consideration.

### ☑ FTC Complaint

File a complaint with the Federal Trade Commission by calling the Identity Theft Hotline (877) 438-4338 or visiting www.ftc.gov/idtheft. The FTC may refer victim complaints to other agencies and companies for further action.

## Fraud Alert

Place a fraud alert on your credit reports. As soon as one of the credit bureaus confirms your fraud alert, the other two credit bureaus will automatically be notified to likewise place fraud alerts on your credit report, and all three reports should be sent to you free of charge.

Once you receive the reports, review them for any discrepancies, unexplained debts on true accounts, inquiries you did not initiate, or accounts you did not open. Contact the bureaus immediately if you notice fraudulent activity on your report(s).

Under the Fair Credit Reporting Act, the credit bureau's investigation must be completed within 30 days (45 days if you provide documents in addition to the ID THEFT Affidavit and a police report). If the bureau considers your dispute frivolous, it must tell you within five business days. Otherwise, it must forward all relevant documents you provide about the dispute to the information provider for further investigation.

Disputed information that cannot be verified must be deleted from your file. If your report contains erroneous information, the credit bureau must correct it. If an item is incomplete, the credit bureau must complete it. If your file shows an account that belongs to someone else, the credit bureau must delete it.

You may add a 100 word victim statement to your credit report which should include your name, telephone number, and an explanation of the problem. This statement may be useful to creditors and law enforcement authorities in their investigation of the identity theft. You may also ask to be contacted by creditors before any new credit is authorized in your name.

The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alert must be made separately at each of the three major credit bureaus.

## Close Accounts

Close any account(s) that has been tampered with or opened fraudulently. Change your password and PIN for replacement accounts. If there are fraudulent charges or debits on your account, ask the company to provide you with the following forms so that you may dispute those transactions.

- For new unauthorized accounts – ask if the company or institution accepts the ID THEFT Affidavit available for free downloads on the Federal Trade Commission's website www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf. If not, ask the representative to send you the company's own fraud dispute form(s).
- For existing accounts – Ask the representative for the company's fraud dispute form(s).

In regard to tampered checks, contact the major check verification companies. Ask that the retailers who use their databases not accept your checks. The major check verification companies are:

- TeleCheck – (800) 710-9898
- Chex Systems – (800) 428-9623
- SCAN – (800) 262-7771
- Equifax – (800) 437-5120
- Cross Check – (800) 552-1900
- CheckRite – (800) 766-2748
- NPC – (800) 526-5380

## Additional Steps You Can Take To Protect Yourself

**Credit Cards**

In most cases, the Truth in Lending Act limits your liability for unauthorized credit card charges to $50 dollars per card. The Fair Credit Billing Act establishes procedures for resolving billing errors. To take advantage of these protections, you must:

- Write to the creditor at the address for "billing inquiries" explaining the problem in detail.
- Send the letter so that it reaches the creditor within 60 days from when the first bill showing the fraudulent charges was mailed to you. Your address being fraudulently changed is not an excuse for not meeting this deadline. Include COPIES of documents that support your claim.
- The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved.
- The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

**ATM/Debit Cards & Electronic Fund Transfers**

The Electronic Fund Transfer Act provides consumer protections for transactions involving electronic methods to debit or credit an account, as well as providing limits to a consumer's liability for unauthorized electronic fund transfers.

It's important to report lost or stolen ATM/debit cards immediately because the amount that you may be responsible for depends on how quickly your report the loss.

- If you report a lost or stolen card within two business days of discovering the loss or theft, your losses are limited to $50 dollars.
- If you report a lost or stolen card after two business days, but within 60 days after a statement showing an unauthorized transfer, you may be liable for up to $500 of what the thief withdraws.
- If you wait more than 60 days, you could lose all the money that was fraudulently withdrawn from your account from the end of the 60 days to the time you report the loss or theft.

*Note*: VISA and MasterCard have voluntarily agreed to cap consumer liability for unauthorized use of their debit cards in most instances to $50 dollars per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

The best way to protect yourself in the event you fall victim to an authorized electronic funds transfer is to contact your financial institution immediately by telephone at first and then follow up with a certified letter, return receipt requested, so that you can document when the institution received your letter.

After receiving notification about an error on your statement, the financial institution generally has 10 business days to investigate the alleged theft. The institution must tell you the result of its investigation within three business days after completing it and must correct an error within one business day after determining that the error has occurred.

If the financial institution needs more time to investigate the theft, it may take up to 45 days to complete the investigation, but only if the money in dispute is returned to your account and you are notified promptly of the credit. After completing its investigation, if no error has been found, the institution may take the credit back if it sends you a written explanation for such action.

**Debt Collectors**

The Fair Debt Collection Practices Act prohibits debts collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection. You can stop a debt collector from contacting you by writing a letter to the collection agency telling them to stop contacting you. A collector also may not contact you if, within 30 days after you receive the collection notice, you send the collection agency a letter that you do not owe the money. Once the debt collector receives your letter, the company may not contact you again – with two exceptions:

- They can tell you there will be no further contact; and
- They can tell you that the debt collector or the creditor intends to take some specific action.

Also, a collector can renew collection activities if they send you proof of the debt. Therefore, include any relevant documentation proving your innocence with your letter to the collector.

**Social Security Number**

If you have done everything possible to fix the problem and your number is still being used fraudulently, you may be assigned a new Social Security Number. There is no guarantee that this will fix the problem however.

Also, please remember that you cannot receive a new Social Security Number if (1) you have filed for bankruptcy, (2) your intention is to avoid the law or legal responsibilities, or (3) your Social Security card has been lost or stolen, but there is no evidence of any misuse.

# Ohio Passport Identification Program

The Ohio Attorney General unveiled the Identity Theft Verification Passport program in December 2004 in order to assist victims of identity theft rehabilitate their good name and credit record. The cornerstone of this unique program is a *PASSPORT* card issued to victims of identity theft which will conclusively demonstrate to law enforcement authorities and creditors alike that their identity has been stolen.

In the unfortunate event that you may become a victim of identity theft, you should immediately file a police report with your local law enforcement agency about your identity being stolen. Once verification of the crime is confirmed, you may apply for the Identity Theft Verification *PASSPORT* card with the assisting law enforcement officer. The whole process should take less than 10 minutes. Note that there is a seven year retroactive limit on identity theft beginning on December 14, 2004, and that only Ohio law enforcement can complete the *PASSPORT* application form.

The *PASSPORT* application has been made available to all Ohioans free of charge through the Ohio Law Enforcement Gateway (OHLEG) at www.ohleg.org – a secure, restricted Internet resource for use by law enforcement agencies statewide. Along with information regarding the police report, the application will contain the victim's personal data (name, address, phone number, driver's license), as well as the victim's fingerprints, photograph and signature made under oath that his/her statements are truthful. Once the application has been submitted, agencies across Ohio will be able to instantly confirm that a person has reported an identity theft via OHLEG.

Upon completing the *PASSPORT* application, the local law enforcement agency will also transmit the application and police report instantaneously to the Attorney General's Office, who in turn will verify said information and thereafter issue a *PASSPORT* card to the victim, which will contain a unique identifier number. The *PASSPORT* card will be sent to the victim who must then activate the card using a number from their *PASSPORT* application by calling (888) MY-ID-4-ME [(888) 694-3463]. In the event that an identity theft victim loses their *PASSPORT* card, the Attorney General's Office will deactivate the lost card and a completely new application and card must be made.

Once activated, creditors and law enforcement officers will be able to verify the validity of the *PASSPORT* card by calling (877) VERIFY-IT, [(877) 837-4394]. Law enforcement officers will also have the benefit of accessing all the information submitted on the *PASSPORT* application, including the original police report and the digitized fingerprint, photograph and signature stored in the OHLEG database. Such security features will undoubtedly help creditors and law enforcement differentiate between the innocent victim of identity theft and the criminal that has made a mess of the victim's life.

For additional information about the *PASSPORT* program, you may call the Attorney General's Office at (888) 694-3463 or else visit his web site at www.ag.state.oh.us.

# Contact Information

## Credit Bureaus

**Equifax**
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
(800) 525-6285

**Experian**
www.experian.com
P.O. Box 9532
Allen, TX 75013
(888) 397-3742

**Trans Union**
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790 Fullerton, CA
92834-6790
(800) 680-7289

## Federal Agencies

**Federal Trade Commission**
www.ftc.gov
ID Theft Clearinghouse, FTC
600 Pennsylvania Avenue, NW
Washington D.C. 20580
(877) 438-4338

**FCC**
www.fcc.gov.cgb.complaints.html
Email – fccinfo@fcc.gov
(888) 225-5322

**Social Security**
www.socialsecurity.gov or
www.ssa.gov/mystatement/
(800) 772-1213

**Secret Service**
www.secretservice.gov
(216) 706-4365 (Cleveland office)

## State and Local Agencies

**Ohio Attorney General**
www.ag.state.oh.us
(800) 282-0515 (Consumer Protection)
(888) 694-3463 (General Number)

**Ohio Consumer Counsel**
www.pickocc.org
Email – occ@occ.state.oh.us
(877) 742-5622

**Parma Police Department**
(440) 887-7300

# General Protection Tips

- ☑ Order a free copy of your credit report by going to www.annualcreditreport.com or calling (877) 322-8228. Do not use www.freecreditreport.com.
- ☑ Register with Direct Marketing Association (DMA) to opt-out of most marketing lists by calling (888) 5 OPTOUT (567-8688) or going to www.dmachoice.org.
  - You may also register with DMA by submitting a registration form to: Mail Preference Service; Attn. Dept. 27478505; Direct Marketing Association; P.O. Box 282; Carmel, New York 10512. Within 90 days of receiving your request, approximately 70% of national direct marketers will delete your name and address from their marketing list. The registration costs $1 and will be good for three years.
- ☑ Stop pre-approved credit card solicitations by calling (888) 567-8688 or by going to www.optoutprescreen.com.
- ☑ Place your address on the Parma "Do Not Knock" registry which effectively prohibits peddlers and solicitors from disturbing residents at their homes. You may register by going to www.cityofparma-oh.gov/donotknock/index.aspx.
- ☑ Remove your name from Telemarketing lists by registering your home telephone or mobile telephone with the National Do Not Call Registry by calling (888) 382-1222 from the telephone you want to register or going to www.donotcall.gov. Registration is effective for five years. Telemarketers have 31 days from the date you register to stop calling you. Violators are subject to fines up to $11,000 per violation. Exempt businesses include:
  - long distance telephone companies;
  - airlines;
  - insurance Companies that operate under state regulations;
  - organizations with which you have a business relationship can call you for up to 18 months after your last transaction;
  - companies to which you have made an inquiry or submitted an application call call you for three months afterwards.
- ☑ Report telemarketing fraud by calling the following numbers:
  - Federal Trade Commission (877) 382-4357 (toll free); (866) 653-4261 (TTY)
  - Ohio Attorney General (216) 787-3030
  - Parma Police Department (440) 887-7300